

THE DIVISOR MATRIX, DIRICHLET SERIES AND $\mathrm{SL}(2, \mathbf{Z})$

PETER SIN AND JOHN G. THOMPSON

ABSTRACT. A representation of $\mathrm{SL}(2, \mathbf{Z})$ by integer matrices acting on the space of analytic ordinary Dirichlet series is constructed, in which the standard unipotent element acts as multiplication by the Riemann zeta function. It is then shown that the Dirichlet series in the orbit of the zeta function are related to it by algebraic equations.

1. INTRODUCTION

This paper is concerned with group actions on the space of analytic Dirichlet series. A *formal* Dirichlet series is a series of the form $\sum_{n=1}^{\infty} a_n n^{-s}$, where $\{a_n\}_{n=1}^{\infty}$ is a sequence of complex numbers and s is formal variable. Such series form an algebra $\mathcal{D}[[s]]$ under the operations of termwise addition and scalar multiplication and multiplication defined by Dirichlet convolution:

$$(1) \quad \left(\sum_{n=1}^{\infty} a_n n^{-s} \right) \left(\sum_{n=1}^{\infty} b_n n^{-s} \right) = \sum_{n=1}^{\infty} \left(\sum_{ij=n} a_i b_j \right) n^{-s}.$$

It is well known that this algebra, sometimes called the *algebra of arithmetic functions*, is isomorphic with the algebra of formal power series in a countably infinite set of variables. The *analytic* Dirichlet series, those which converge for some complex value of the variable s , form a subalgebra $\mathcal{D}\{s\}$, shown in [6] to be a local, non-noetherian unique factorization domain. As a vector space we can identify $\mathcal{D}[[s]]$ with the space of sequences and $\mathcal{D}\{s\}$ with the subspace of sequences satisfying a certain polynomial growth condition. It is important for our purposes that the space of sequences is the dual E^* of a space E of countable dimension, since the linear operators on $\mathcal{D}\{s\}$ of interest to us are induced from operators on E . We take E to be the space of columns, indexed by positive integers, which have only finitely many nonzero entries. In the standard basis of E , endomorphisms acting on the left are represented by column-finite matrices with rows and columns indexed by the positive integers. They act on E^* by right multiplication. The endomorphisms of E which preserve $\mathcal{D}\{s\}$ in their right action form a subalgebra \mathcal{DR} . There is a natural embedding of $\mathcal{D}\{s\}$ into \mathcal{DR} mapping a series to the *multiplication operator* defined by convolution with the series. The Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, $\text{Re}(s) > 1$, is mapped to the *divisor matrix* $D = (d_{i,j})_{i,j \in \mathbf{N}}$, defined by

$$d_{i,j} = \begin{cases} 1, & \text{if } i \text{ divides } j, \\ 0 & \text{otherwise.} \end{cases}$$

It is also of interest to study noncommutative subalgebras of \mathcal{DR} or nonabelian subgroups of \mathcal{DR}^\times which contain D . In [5], it was shown that $\langle D \rangle$ could be embedded as the cyclic subgroup of index 2 in an infinite dihedral subgroup of \mathcal{DR}^\times . Given a group G , the problem of finding a subgroup of \mathcal{DR}^\times isomorphic with G and containing D is equivalent to the problem of finding a matrix representation of G into \mathcal{DR}^\times in which some group element is represented by D .

As a reduction step for this general problem, it is desirable to transform the divisor matrix into a Jordan canonical form. Since \mathcal{DR} is neither closed under matrix inversion nor similarity, so such a reduction is useful only if the transition matrices belong to \mathcal{DR}^\times . We show explicitly (Lemma 4.5 and Theorem 4.8) that D can be transformed to a Jordan canonical form by matrices in \mathcal{DR}^\times with integer entries.

The remainder of the paper is devoted to the group $G = \mathrm{SL}(2, \mathbf{Z})$. We consider the problem of constructing a representation $\rho : G \rightarrow \mathcal{DR}^\times$ such that the standard unipotent element $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is represented by D and such that an element of order 3 acts without fixed points. The precise statement of the solution of this problem is Theorem 3.1 below. Roughly speaking, the result on the Jordan canonical form reduces the problem to one of constructing a representation of G in which T is represented by a standard infinite Jordan block. In the simplified problem the polynomial growth condition on the matrices representing group elements becomes a certain exponential growth condition and the fixed-point-free condition is unchanged. The construction is the content of Theorem 5.1. Since the group G has few relations it is relatively easy to define matrix representations satisfying the growth and fixed-point-free conditions and with T acting indecomposably. However, the growth condition is not in general preserved under similarity and it is a more delicate matter to find such a representation for which one can prove that the matrix representing T can be put into Jordan form by transformations preserving the growth condition.

As we have indicated, the construction of the representation ρ involves making careful choices and we do not know of an abstract characterization of ρ as a matrix representation. The $\mathbf{C}G$ -module affording ρ can, however, be characterized as the direct sum of isomorphic indecomposable modules where the isomorphism type of the summands is uniquely determined up to $\mathbf{C}G$ -isomorphism by the indecomposable action of T and the existence of a filtration by standard 2-dimensional modules (Theorem 8.1). Although ρ is just one among many matrix representations of G into \mathcal{DR}^\times which satisfy our conditions, we proceed to examine the orbit of $\zeta(s)$ under $\rho(G)$. We find (Theorem 10.2) that one series $\varphi(s)$ in this orbit is related to $\zeta(s)$ by the cubic equation

$$(2) \quad (\zeta(s) - 1)\varphi(s)^2 + \zeta(s)\varphi(s) - \zeta(s)(\zeta(s) - 1) = 0.$$

We also show (Theorem 9.1) that, as a consequence of relations in the image of the group algebra, the other series in the orbit belong to $\mathbf{C}(\zeta(s), \varphi(s))$.

The cubic equation may be rewritten as

$$(3) \quad -\varphi(s) = (\zeta(s) - 1)(\varphi(s)^2 + \varphi(s) - \zeta(s)).$$

The second factor on the right is a unit in $\mathcal{D}\{s\}$, so φ and $\zeta(s) - 1$ are associate irreducible elements in the factorial ring $\mathcal{D}\{s\}$. The fact that there is a cubic equation relating $\zeta(s)$ and an associate of $\zeta(s) - 1$ should be contrasted with the classical theorem of Ostrowski [7], which states that $\zeta(s)$ does not satisfy any algebraic differential-difference equation.

Matrices resembling finite truncations of the divisor matrix were studied by Redheffer in [8]. For each natural number n he considered the matrix obtained from the upper left $n \times n$ submatrix of D by setting each entry in the first column equal to 1. Research on Redheffer's matrices has been motivated by the fact that their determinants are the values of Mertens' function, which links them directly to the Riemann Hypothesis. (See [11], [9] and [10].)

2. BASIC DEFINITIONS AND NOTATION

Let \mathbf{N} denote the natural numbers $\{1, 2, \dots\}$ and \mathbf{C} the complex numbers. Let E be the free \mathbf{C} -module with basis $\{e_n\}_{n \in \mathbf{N}}$. With respect to this basis the endomorphism ring $\text{End}_{\mathbf{C}}(E)$, acting on the left of E , becomes identified with the ring \mathcal{A} of matrices $A = (a_{i,j})_{i,j \in \mathbf{N}}$, with complex entries, such that each column has only finitely many nonzero entries. The dual space E^* becomes identified with the space $\mathbf{C}^{\mathbf{N}}$ of sequences of complex numbers, with $f \in E^*$ corresponding to the sequence $(f(e_n))_{n \in \mathbf{N}}$. We will write $(f(e_n))_{n \in \mathbf{N}}$ as f and $f(e_n)$ as $f(n)$ for short.

In this notation the natural right action of $\text{End}_{\mathbf{C}}(E)$ on E^* is expressed as a right action of \mathcal{A} on $\mathbf{C}^{\mathbf{N}}$ by

$$(fA)(n) = \sum_{m \in \mathbf{N}} a_{m,n} f(m), \quad f \in \mathbf{C}^{\mathbf{N}}, A \in \mathcal{A}.$$

(The sum has only finitely many nonzero terms.)

Let \mathcal{DS} be the subspace of $\mathbf{C}^{\mathbf{N}}$ consisting of the sequences f for which there exist positive constants C and c such that for all n , $|f(n)| \leq Cn^c$. A sequence f lies in \mathcal{DS} if and only if the Dirichlet series $\sum_n f(n)n^{-s}$ converges for some complex number s , which gives a canonical bijection between \mathcal{DS} and the space $\mathcal{D}\{s\}$ of analytic Dirichlet series. Let \mathcal{DR} be the subalgebra of \mathcal{A} consisting of all elements which leave \mathcal{DS} invariant.

A sufficient condition for membership in \mathcal{DR} is provided by the following lemma, whose proof is straightforward.

Lemma 2.1. *Let $A = (a_{i,j})_{i,j \in \mathbf{N}} \in \mathcal{A}$. Suppose that there exist positive constants C and c such that the following hold.*

- (i) $a_{i,j} = 0$ whenever $i > Cj^c$.
- (ii) For all i and j we have $|a_{i,j}| \leq Cj^c$.

Then $A \in \mathcal{DR}$. Furthermore, the set of all elements of \mathcal{A} which satisfy these conditions, where the constants may depend on the matrix, is a subring of \mathcal{DR} .

We let \mathcal{DR}_0 denote the subring of \mathcal{DR} defined by the lemma. If $\sum_{n \in \mathbf{N}} f(n)n^{-s} \in \mathcal{D}\{s\}$, then its multiplication operator has matrix with (i, ni) entries equal to $f(n)$ for all i and n and all other entries zero, so the multiplication operators form commutative subalgebra of \mathcal{DR}_0 .

Remarks 2.2. There exist elements of \mathcal{DR} which do not satisfy the hypotheses of Lemma 2.1. An example is the matrix $(a_{i,j})_{i,j \in \mathbf{N}}$ defined by

$$a_{i,j} = \begin{cases} \frac{1}{j^{j^2}}, & \text{if } i = j^j, \\ 0, & \text{otherwise.} \end{cases}$$

There are invertible matrices in \mathcal{DR}_0 whose inverses are not in \mathcal{DR} . For example, the matrix $(b_{i,j})_{i,j \in \mathbf{N}}$, given by

$$b_{i,j} = \begin{cases} 0, & \text{if } i > j, \\ 1, & \text{if } i = j, \\ -1 & \text{if } i < j \end{cases}$$

is obviously in \mathcal{DR}_0 , while its inverse, given by

$$b'_{i,j} = \begin{cases} 0, & \text{if } i > j, \\ 1, & \text{if } i = j, \\ 2^{j-i-1} & \text{if } i < j \end{cases}$$

is not in \mathcal{DR} .

3. AN ACTION OF $\mathrm{SL}(2, \mathbf{Z})$ ON DIRICHLET SERIES

The group $G = \mathrm{SL}(2, \mathbf{Z})$ is generated by the matrices

$$(4) \quad S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

These matrices satisfy the relations

$$(5) \quad S^4 = (ST)^6 = 1, \quad S^2 = (ST)^3$$

which, as is well known, form a set of defining relations for $\mathrm{SL}(2, \mathbf{Z})$ as an abstract group.

With the above definitions, we can state one of our principal results.

Theorem 3.1. *There exists a representation $\rho : \mathrm{SL}(2, \mathbf{Z}) \rightarrow \mathcal{A}^\times$ with the following properties.*

(a) *The underlying $\mathbf{C} \mathrm{SL}(2, \mathbf{Z})$ -module E has an ascending filtration*

$$0 = E_0 \subset E_1 \subset E_2 \subset \cdots$$

of $\mathbf{C} \mathrm{SL}(2, \mathbf{Z})$ -submodules such that for each $i \in \mathbf{N}$, the quotient module E_i/E_{i-1} is isomorphic to the standard 2-dimensional $\mathbf{C} \mathrm{SL}(2, \mathbf{Z})$ -module.

(b) $\rho(T) = D$.

(c) $\rho(Y)$ is an integer matrix for every $Y \in \mathrm{SL}(2, \mathbf{Z})$.

(d) $\rho(\mathrm{SL}(2, \mathbf{Z})) \subseteq \mathcal{DR}_0$.

The facts needed for the proof of Theorem 3.1 are established in the following sections and the proof is completed in Section 6.

4. A JORDAN FORM OF THE DIVISOR MATRIX

For $m, k \in \mathbf{N}$, let

$$A_k(m) = \{(m_1, m_2, \dots, m_k) \in (\mathbf{N} \setminus \{1\})^k \mid m_1 m_2 \cdots m_k = m\}$$

and let $\alpha_k(m) = |A_k(m)|$.

The following properties of these numbers follow from the definitions.

Lemma 4.1. (a) $\alpha_k(1) = 0$.

(b) $\alpha_k(m) = 0$ if $m < 2^k$ and $\alpha_k(2^k) = 1$.

(c)

$$(\zeta(s) - 1)^k = \sum_{m=2^k}^{\infty} \frac{\alpha_k(m)}{m^s}.$$

By considering the first $k - 1$ entries of elements of $A_k(m)$, we see that for $k > 1$, we have

$$(6) \quad \alpha_k(m) = \left(\sum_{d|m} \alpha_{k-1}(d) \right) - \alpha_{k-1}(m).$$

Induction yields the following formula.

Lemma 4.2.

$$(7) \quad \sum_{i=1}^{k-1} (-1)^{k-1-i} \sum_{d|m} \alpha_i(d) = \alpha_k(m) + (-1)^k \alpha_1(m).$$

Lemma 4.3. *There exists a constant c such that $\alpha_k(m) \leq m^c$ for all k and m .*

Proof. We choose c with $\zeta(c) = 2$. We proceed by induction on k . Since $\alpha_1(m) \leq 1$, the result is true when $k = 1$. Suppose for some k we have that for all m ,

$$\alpha_k(m) \leq m^c.$$

Then by (6) we have

$$\alpha_{k+1}(m) \leq \sum_{\substack{d|m \\ 1 < d < m}} \alpha_k(m/d) \leq m^c \sum_{\substack{d|m \\ 1 < d < m}} d^{-c} \leq m^c(\zeta(c) - 1) = m^c,$$

which completes the inductive proof. \square

Remark 4.4. Since $\zeta(2) = \pi^2/6$, the constant c can be chosen from the real interval $(1, 2)$.

Let $J = (J_{i,j})_{i,j \in \mathbf{N}}$ be the matrix defined by

$$J_{i,j} = \begin{cases} 1, & \text{if } j \in \{i, 2i\}, \\ 0 & \text{otherwise.} \end{cases}$$

Let $Z = (\alpha(i, j))_{i,j \in \mathbf{N}}$ be the matrix described in the following way. The odd rows have a single nonzero entry, equal to 1 on the diagonal. Let $i = 2^k d$ with d odd. Then the i^{th} row of Z is equal to the d^{th} row of $(D - I)^k$.

Lemma 4.5. *The matrix Z has the following properties:*

- (a) $\alpha(i, j) = \delta_{i,j}$, if i is odd.
- (b) If $i = d2^k$, where d is odd and $k \geq 1$, then

$$\alpha(i, j) = \begin{cases} \alpha_k(j/d) & \text{if } d \mid j, \\ 0 & \text{otherwise.} \end{cases}$$

- (c) $\alpha(im, jm) = \alpha(i, j)$ whenever m is odd.
- (d) Z is upper unitriangular.
- (e) $ZDZ^{-1} = J$.
- (f) $Z \in \mathcal{DR}_0$.

Moreover, Z is the unique matrix satisfying (a) and (e).

Proof. Part (a) is by definition. Part (b) follows from Lemma 4.1(c) upon multiplying by the Dirichlet series with one term d^{-s} . Part (c) is a special case of (b). Part (d) also follows from (b). Part (f) is then immediate from Lemma 4.3. In the equation

$$(8) \quad Z(D - I) = (J - I)Z$$

the n^{th} row of each side is equal to the $2n^{\text{th}}$ row of Z . This proves (e) since Z is invertible by (d). To prove the last statement we see that if (e) holds then by (8) we have for all i and $k \in \mathbf{N}$,

$$\sum_{\substack{j|k \\ j < k}} \alpha(i, j) = \alpha(2i, k),$$

which determines Z uniquely since the rows with odd index are specified by (a). \square

Our aim is to determine Z^{-1} explicitly.

For each prime p and each integer m let $v_p(m)$ denote the exponent of the highest power of p which divides m and let $v(m) = \sum_p v_p(m)$.

Lemma 4.6. *We have for all $m \in \mathbf{N}$,*

$$\sum_{k=1}^{v(m)} (-1)^k \alpha_k(m) = \begin{cases} (-1)^{v(m)}, & \text{if } m \text{ is squarefree and } m > 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The case $m = 1$ is trivial. Suppose $m = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r}$, with $\lambda_1, \lambda_2, \dots, \lambda_r \geq 1$ and $r \geq 1$. In the ring of formal power series $\mathbf{C}[[t_1, \dots, t_r]]$ in r indeterminates we set

$$\begin{aligned} (9) \quad y &= \frac{1}{(1-t_1)(1-t_2)\cdots(1-t_r)} - 1 \\ &= \sum_{(n_1, \dots, n_r) \in (\mathbf{N} \cup \{0\})^r} \alpha_1(p_1^{n_1} \cdots p_r^{n_r}) t_1^{n_1} \cdots t_r^{n_r}. \end{aligned}$$

Then for $k \geq 1$

$$(10) \quad y^k = \sum_{(n_1, \dots, n_r) \in (\mathbf{N} \cup \{0\})^r} \alpha_k(p_1^{n_1} \cdots p_r^{n_r}) t_1^{n_1} \cdots t_r^{n_r}.$$

Then we have

$$\begin{aligned} (11) \quad \prod_{i=1}^r (1-t_i) - 1 &= \frac{-y}{1+y} \\ &= \sum_{k \in \mathbf{N}} (-1)^k y^k \\ &= \sum_{(n_1, \dots, n_r) \in (\mathbf{N} \cup \{0\})^r} \left[\sum_{k \in \mathbf{N}} (-1)^k \alpha_k(p_1^{n_1} \cdots p_r^{n_r}) \right] t_1^{n_1} \cdots t_r^{n_r}. \end{aligned}$$

The lemma follows by equating the coefficients of monomials. \square

Remark 4.7. The above proof is similar to the argument in [1], p.21, used to show that $\sum_k (-1)^k \alpha_k(m)/k$ is equal to $1/h$ if m is the h -th power of a prime, and zero otherwise. The lemma has also the following enumerative proof, based on another combinatorial interpretation of the sets $A_k(m)$. From the above factorization of m let λ be the partition of n defined by the λ_i . Let $N = \{1, \dots, n\}$ and let F_λ be the set of functions $h : N \rightarrow \{p_1, \dots, p_r\}$ such that $|h^{-1}(p_i)| = \lambda_i$ for $i = 1, \dots, r$. The symmetric group S_n acts transitively on the right of F_λ by the rule $(h\sigma)(y) = h(\sigma(y))$, $y \in N$, $\sigma \in S_n$. The stabilizer S_λ of the function mapping the first λ_1 elements to p_1 , the next λ_2 elements to p_2 , etc. is isomorphic to $S_{\lambda_1} \times S_{\lambda_2} \times \dots \times S_{\lambda_r}$. A k -decomposition of n is a k -tuple (n_1, \dots, n_k) of integers $n_i \geq 1$ such that $n_1 + n_2 + \dots + n_k = n$. Let $\Pi = \{\sigma_1, \dots, \sigma_{n-1}\}$ be the set of fundamental reflections, with $\sigma_i = (i, i+1)$. The subgroup W_K of S_n generated by a subset K of Π is called a standard parabolic subgroup of rank $|K|$. Given a k -decomposition (n_1, \dots, n_k) of n , we have a set decomposition of N into subsets $N_1 = \{1, \dots, n_1\}$, $N_2 = \{n_1 + 1, \dots, n_1 + n_2\}$, \dots , $N_k = \{n_1 + \dots + n_{k-1} + 1, \dots, n\}$. The stabilizer of this decomposition is a standard parabolic subgroup of rank $n - k$ and this correspondence is a bijection between k -decompositions and standard parabolic subgroups of rank $n - k$.

For each pair $((n_1, \dots, n_k), h)$ consisting of a k -decomposition and a function $h \in F_\lambda$, we obtain an element $(m_1, \dots, m_k) \in A_k(m)$ by setting $m_i = \prod_{j \in N_i} h(j)$. Every element of $A_k(m)$ arises in this way and two pairs define the same element of $A_k(m)$ if and only if the k -decompositions are equal and the corresponding functions are in the same orbit under the action of the parabolic subgroup of the k -decomposition.

Thus, we have

$$\alpha_k(m) = |A_k(m)| = \sum_{\substack{K \subseteq \Pi \\ |K|=n-k}} |\{W_K\text{-orbits on } F_\lambda\}|.$$

The number of W_K -orbits on F_λ can be expressed as the inner product of permutation characters, so

$$\alpha_k(m) = \sum_{\substack{K \subseteq \Pi \\ |K|=n-k}} \langle 1_{W_K}^{S_n}, 1_{S_\lambda}^{S_n} \rangle.$$

Now, it is a well known fact [2] that

$$\sum_{K \subseteq \Pi} (-1)^{|K|} 1_{W_K}^{S_n} = \epsilon,$$

where ϵ is the sign character. Hence,

$$\begin{aligned}
\sum_{k=1}^n (-1)^k \alpha_k(m) &= (-1)^n \left\langle \sum_{K \subseteq \Pi} (-1)^{|K|} 1_{W_K}^{S_n}, 1_{S_\lambda}^{S_n} \right\rangle \\
&= (-1)^n \langle \epsilon, 1_{S_\lambda}^{S_n} \rangle \\
&= (-1)^n \langle \epsilon, 1 \rangle_{S_\lambda} \\
&= \begin{cases} (-1)^n, & \text{if } \lambda = 1^n, \\ 0, & \text{otherwise.} \end{cases}
\end{aligned}$$

Let X be the diagonal matrix with (i, i) entry equal to $(-1)^{v_2(i)}$, for $i \in \mathbf{N}$.

Theorem 4.8. $Z^{-1} = XZX$. In particular, $Z^{-1} \in \mathcal{DR}_0$.

Proof. If i is odd then the i^{th} row of Z is zero except for 1 in the i^{th} column, so the same holds for XZX . By the last assertion of Lemma 4.5 it is sufficient to show that

$$D(XZX) = (XZX)J$$

or, equivalently,

$$(XDX)Z = Z(XJX).$$

The matrices $XDX = (d'_{i,j})_{i,j \in \mathbf{N}}$ and $XJX = (c'_{i,j})_{i,j \in \mathbf{N}}$ are given by

$$d'_{i,j} = \begin{cases} (-1)^{v_2(i)+v_2(j)}, & \text{if } i \mid j, \\ 0 & \text{otherwise.} \end{cases}, \quad c'_{i,j} = \begin{cases} 1, & \text{if } j = i, \\ -1, & \text{if } j = 2i, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, we must show that

$$(12) \quad \sum_{m \geq 1} (-1)^{v_2(m)} \alpha(im, j) = \begin{cases} \alpha(i, j), & \text{if } j \text{ is odd,} \\ \alpha(i, j) - \alpha(i, j/2), & \text{if } j \text{ is even.} \end{cases}$$

It is sufficient to consider the case $i = 2^k$, for $k \geq 1$, by Lemma 4.5(c). In this case, the left hand side of (12) can be rewritten as

$$\begin{aligned}
(13) \quad & \sum_{\substack{d \mid j \\ d \text{ odd}}} \sum_{e=0}^{v(j)-k-v(d)} (-1)^e \alpha(2^{k+e}, j/d) \\
&= (-1)^k \sum_{\substack{d \mid j \\ d \text{ odd}}} \sum_{r=k}^{v(j/d)} (-1)^r \alpha(2^r, j/d).
\end{aligned}$$

Suppose that we can prove for all j , that

$$(14) \quad (-1)^k \sum_{d|j} \sum_{r=k}^{v(j/d)} (-1)^r \alpha(2^r, j/d) = \alpha(2^k, j).$$

Then we will have proved (12) if j is odd. If j is even, we note that d is a divisor of $j/2$ if and only if $2d$ is an even divisor of j , so that (14) implies

$$\begin{aligned} \alpha(2^k, j/2) &= (-1)^k \sum_{d|(j/2)} \sum_{r=k}^{v((j/2)/d)} (-1)^r \alpha(2^r, (j/2)/d) \\ &= (-1)^k \sum_{\substack{d'|j \\ d' \text{ even}}} \sum_{r=k}^{v(j/d')} (-1)^r \alpha(2^r, j/d'). \end{aligned}$$

Thus, from (13) we see that (12) also follows from (14) when j is even. It remains to prove (14). We can assume $j > 1$, by Lemma 4.1(a). Lemma 4.6, applied to the left hand side of (14), yields

$$(15) \quad (-1)^{k-1} + (-1)^{k-1} \sum_{d|j} \left(\sum_{r=1}^{k-1} (-1)^r \alpha_r(j/d) \right)$$

because the total contribution from the squarefree case of Lemma 4.6 is

$$(-1)^k \sum_{\substack{d|j \\ j/d \text{ squarefree} \\ j/d > 1}} (-1)^{v(j/d)} = (-1)^{k-1}.$$

We can rewrite (15) as

$$(-1)^{k-1} + \sum_{r=1}^{k-1} (-1)^{k-1-r} \sum_{d|j} \alpha_r(d),$$

which, by Lemma 4.2 is equal to $\alpha_k(j)$. This proves (14). \square

5. CONSTRUCTION OF REPRESENTATIONS

Let J_∞ be the “infinite Jordan block”, indexed by $\mathbf{N} \times \mathbf{N}$, defined by

$$(J_\infty)_{i,j} = \begin{cases} 1, & \text{if } j = i \text{ or } j = i + 1, \\ 0 & \text{otherwise.} \end{cases}$$

In the following theorem, T and S are the generators of $\mathrm{SL}(2, \mathbf{Z})$ defined in (4).

Theorem 5.1. *There exists a representation $\tau : \mathrm{SL}(2, \mathbf{Z}) \rightarrow \mathcal{A}^\times$ with the following properties.*

- (a) *Let E_i be the subspace of E spanned by $\{e_1, \dots, e_{2i}\}$, $i \in \mathbf{N}$. Then*

$$0 = E_0 \subset E_1 \subset E_2 \subset \dots$$

is a filtration of $\mathbf{C} \mathrm{SL}(2, \mathbf{Z})$ -modules and for each $i \in \mathbf{N}$ the quotient module E_i/E_{i-1} is isomorphic to the standard 2-dimensional $\mathbf{C} \mathrm{SL}(2, \mathbf{Z})$ -module.

- (b) $\tau(T) = J_\infty$.
(c) $\tau(Y)$ is an integer matrix for every $Y \in \mathrm{SL}(2, \mathbf{Z})$.
(d) *There is a constant C such that for all i and j we have $|\tau(S)_{i,j}| \leq 2^{Cj}$.*

Later we will show (Theorem 8.1) that there is a unique $\mathbf{C} \mathrm{SL}(2, \mathbf{Z})$ -module with a filtration by standard modules and such that T acts indecomposably and unipotently on every T -invariant subspace.

We define a sequence of integers $\{b_n\}_{n \geq 0}$ recursively by¹

$$(16) \quad b_0 = b_1 = 1, \quad b_n + \sum_{\substack{i,j \geq 1 \\ i+j=n}} b_i b_j = 0 \quad \text{for all } n \geq 2.$$

Let $\mathbf{C}[[t]]$ denote the ring of formal power series over \mathbf{C} and let $g(t) \in \mathbf{C}[[t]]$ be defined by

$$1 + g(t) = \sum_{k=0}^{\infty} b_k t^k.$$

Then the recurrence relations satisfied by the b_i can be stated as the equation

$$(17) \quad g(t)^2 + g(t) = t.$$

Thus,

$$g(t) = \frac{-1 + \sqrt{1 + 4t}}{2},$$

where the positive square root is taken since $g(t)$ has no constant term. By Taylor expansion we obtain

$$(18) \quad b_m = \frac{(-1)^{m-1}}{m} \binom{2m-2}{m-1}, \quad (m \geq 2), \quad b_1 = b_0 = 1.$$

¹As J-P. Serre has pointed out to us, this is the sequence of Catalan numbers, up to signs.

Let

$$B_0 = T, \quad B_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad B_i = \begin{bmatrix} 0 & b_i \\ b_i & 0 \end{bmatrix}, \quad (i \geq 2)$$

and define

$$\tilde{J} = \begin{bmatrix} B_0 & B_1 & B_2 & B_3 & \dots \\ 0 & B_0 & B_1 & B_2 & \dots \\ 0 & 0 & B_0 & B_1 & \dots \\ 0 & 0 & 0 & B_0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix},$$

$$\tilde{S} = \mathrm{diag}(S, S, \dots),$$

$$\tilde{R} = -\tilde{S}\tilde{J}.$$

For any ring R let $M_n(R)$ denote the ring of $n \times n$ matrices over R . Let \mathcal{U} denote the ring of matrices of the form

$$(19) \quad U = \begin{bmatrix} X^{(0)} & X^{(1)} & X^{(2)} & X^{(3)} & \dots \\ 0 & X^{(0)} & X^{(1)} & X^{(2)} & \dots \\ 0 & 0 & X^{(0)} & X^{(1)} & \dots \\ 0 & 0 & 0 & X^{(0)} & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix},$$

where, for all $n \geq 0$,

$$X^{(n)} = \begin{bmatrix} x_{1,1}^{(n)} & x_{1,2}^{(n)} \\ x_{2,1}^{(n)} & x_{2,2}^{(n)} \end{bmatrix} \in M_2(\mathbf{C})$$

and the $X^{(n)}$ are repeated down the diagonals. For example, \tilde{S} , \tilde{J} and \tilde{R} all belong to \mathcal{U} . The center $Z(\mathcal{U})$ consists of those matrices in which the submatrices $X^{(n)}$ are all scalar matrices. The map $\mathbf{C}[[t]] \rightarrow Z(\mathcal{U})$ sending $\sum_{n \geq 0} a_n t^n$ to the matrix with $X^{(n)} = a_n I$, for all $n \geq 0$, is a \mathbf{C} -algebra isomorphism, and extends to a $\mathbf{C}[[t]]$ -algebra isomorphism

$$(20) \quad \gamma : \mathcal{U} \rightarrow M_2(\mathbf{C}[[t]]), \quad U \mapsto \begin{bmatrix} x_{1,1}(t) & x_{1,2}(t) \\ x_{2,1}(t) & x_{2,2}(t) \end{bmatrix},$$

where

$$x_{i,j}(t) = \sum_{n=0}^{\infty} x_{i,j}^{(n)} t^n, \quad i, j \in \{1, 2\}.$$

We have:

(21)

$$\gamma(\tilde{S}) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \gamma(\tilde{J}) = \begin{bmatrix} 1 & 1+g(t) \\ g(t) & 1+t \end{bmatrix}, \quad \gamma(\tilde{R}) = \begin{bmatrix} g(t) & 1+t \\ -1 & -1-g(t) \end{bmatrix}.$$

Lemma 5.2. (a) $\tilde{S}^2 = -I$.

(b) $\tilde{R}^2 + \tilde{R} + I = 0$.

(c) *There exists a representation τ_1 of G such that $\tau_1(S) = \tilde{S}$ and $\tau_1(T) = \tilde{J}$.*

Proof. Part (a) is obvious and (b) is easy to check by direct computation using (21) and (17). By (a) and (b), the elements \tilde{S} and \tilde{J} satisfy the defining relations (5) for $\text{SL}(2, \mathbf{Z})$, so (c) holds. \square

The representation τ_1 satisfies all the conditions of Theorem 5.1 except for (b). To complete the proof of Theorem 5.1 we shall conjugate this representation by an upper unitriangular integer matrix P such that $P\tilde{J}P^{-1} = J_\infty$. In order to check that $P\tilde{S}P^{-1}$ satisfies condition (d) of Theorem 5.1 we will need to compute P and its inverse explicitly.

5.1. Transforming \tilde{J} into Jordan form. A matrix P such that $P\tilde{J}P^{-1} = J_\infty$ can be found by following the usual method for computing Jordan blocks. Thus, for $n \in \mathbf{N}$, we define the n^{th} row of P to be the first row of $(\tilde{J} - I)^{n-1}$, setting $(\tilde{J} - I)^0 = I$. Then P is upper unitriangular, hence invertible, and, from its definition, P satisfies the equivalent equation

$$P(\tilde{J} - I) = (J_\infty - I)P.$$

We now compute the entries of P explicitly. In order to do this, we use the isomorphism γ of (20). Let $\tilde{H} = \gamma(\tilde{J} - I)$. Then

$$\tilde{H} = \begin{bmatrix} 0 & 1+g(t) \\ g(t) & t \end{bmatrix}.$$

It is easy to compute the powers of $\tilde{J} - I$ by diagonalizing \tilde{H} . Since $g(t)^2 + g(t) = t$, the characteristic polynomial of \tilde{H} is $\chi(x) = x^2 - tx - t$. Let λ_1 and λ_2 be the roots of this polynomial in some extension field and for $n \geq 0$ let $h_n = (\lambda_1^{n+1} - \lambda_2^{n+1})/(\lambda_1 - \lambda_2)$ be the complete symmetric polynomial of degree n in two variables, evaluated at (λ_1, λ_2) . Then h_n is a polynomial in the coefficients of $\chi(x)$, so it is a polynomial in t . We have $h_0 = 1$ and $h_1 = t$. A straightforward computation shows that, for $n \geq 2$,

$$(22) \quad \tilde{H}^n = \begin{bmatrix} th_{n-2} & (1+g(t))h_{n-1} \\ g(t)h_{n-1} & h_n \end{bmatrix}.$$

It follows from (22) and the equation $g(t)^2 + g(t) = t$ that the polynomials h_n satisfy the recurrence

$$h_n = th_{n-1} + th_{n-2}, \quad (n \geq 2), \quad h_0 = 1, \quad h_1 = t.$$

By inspection, the solution is

$$h_n = \sum_{r=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-r}{r} t^{n-r}.$$

Thus we can compute the entries of P as coefficients of the powers of t in the top rows of the \tilde{H}^n . For $\ell \geq 3$ and $s \geq 0$, we have

$$\begin{aligned} p_{\ell, 2s+1} &= \text{coefficient of } t^s \text{ in } th_{\ell-3} \\ &= \binom{s-1}{\ell-s-2}, \\ (23) \quad p_{\ell, 2s+2} &= \text{coefficient of } t^s \text{ in } (1+g(t))h_{\ell-2} \\ &= \sum_{k=0}^{\lfloor s+1-\frac{\ell}{2} \rfloor} b_k \binom{s-k}{\ell+k-s-2}. \end{aligned}$$

Here and elsewhere, we employ the convention for binomial coefficients that $\binom{a}{b} = 0$ unless $a \geq b \geq 0$.

We now turn to the computation of P^{-1} . Suppose a matrix $Q = (q_{i,j})_{i,j \in \mathbf{N}}$ satisfies the two conditons

$$(24) \quad \tilde{J}Q = QJ_\infty \quad \text{and} \quad q_{1,j} = \delta_{1,j}.$$

The first conditon implies that PQ commutes with J_∞ and the second that $(PQ)_{1,j} = \delta_{1,j}$, from which it follows that $PQ = I$ and $Q = P^{-1}$. We find a matrix Q satisfying (24) by first finding a matrix A such that

$$(25) \quad (\tilde{J} - I)A = A(J_\infty - I)$$

and then modifying it. To compute A we must first enlarge the ring \mathcal{U} . Let $\hat{\mathcal{U}}$ denote the set of matrices of the form

$$W = \begin{bmatrix} \dots & X^{(m)} & X^{(m+1)} & X^{(m+2)} & X^{(m+3)} & \dots \\ \dots & X^{(m-1)} & X^{(m)} & X^{(m+1)} & X^{(m+2)} & \dots \\ \dots & X^{(m-2)} & X^{(m-1)} & X^{(m)} & X^{(m+1)} & \dots \\ \dots & X^{(m-3)} & X^{(m-2)} & X^{(m-1)} & X^{(m)} & \dots \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \end{bmatrix},$$

where the blocks $X^{(m)} \in M_2(\mathbf{C})$, for $m \in \mathbf{Z}$, are repeated down the diagonals and have the property that for some $m_0 \in \mathbf{Z}$, which may depend on W , $X^{(m)} = 0$ whenever $m < m_0$. We shall refer to the

two columns of W headed by $X^{(m)}$ as the $[m, 1]$ column and the $[m, 2]$ column, respectively. For $W \in \widehat{\mathcal{U}}$ and $m \in \mathbf{Z}$, we denote by $W(m)$ the submatrix of W whose first column is the $[m, 1]$ column of W . To be concise, we can write $W = (X^{(m)})_{m \in \mathbf{Z}}$, since the top row determines the whole matrix. A product is defined as follows. Let $W' = (Y^{(m)})_{m \in \mathbf{Z}} \in \widehat{\mathcal{U}}$. Then $WW' = (Z^{(m)})_{m \in \mathbf{Z}}$, where

$$Z^{(m)} = \sum_{i+j=m} X^{(i)} Y^{(j)}.$$

This product can be computed as an ordinary matrix product as follows. Let m_0 and n_0 be chosen such that $X^{(m)} = 0$ for all $m < m_0$ and $Y^{(n)} = 0$ for all $n < n_0$. Then WW' is obtained from the ordinary matrix product $W(m_0)W'(n_0)$ by adjoining columns of zeros to the left and declaring the first column of $W(m_0)W'(n_0)$ to be the $[m_0 + n_0, 1]$ column of the new matrix. The answer is independent of the choice of m_0 and n_0 , due to the diagonal pattern of elements of $\widehat{\mathcal{U}}$. Together with the usual vector space structure on matrices, the above product makes $\widehat{\mathcal{U}}$ into a \mathbf{C} -algebra. The subset of elements $W \in \widehat{\mathcal{U}}$ such that $X^{(m)} = 0$ for all $m < 0$ forms a subalgebra isomorphic to the algebra \mathcal{U} defined in (19). Let $\mathbf{C}((t))$ denote the field of formal Laurent series, the field of fractions of $\mathbf{C}[[t]]$. The center $Z(\widehat{\mathcal{U}})$ consists of the elements in which all the submatrices $X^{(m)}$ are scalar. The map sending the Laurent series $\sum_n a_n t^n$ to the element $(X^{(m)})_{m \in \mathbf{Z}}$ such that $X^{(m)} = a_m I$ for all m , is an isomorphism of $\mathbf{C}((t))$ with $Z(\widehat{\mathcal{U}})$. This extends to an isomorphism of $\mathbf{C}((t))$ -algebras

$$\widehat{\gamma} : \widehat{\mathcal{U}} \rightarrow M_2(\mathbf{C}((t))),$$

which is the unique extension of the isomorphism (20).

Now, the element $\tilde{J} - I$ is invertible in $\widehat{\mathcal{U}}$, since $\tilde{H} = \widehat{\gamma}(\tilde{J} - I)$ has determinant $-t$. We define $A = (a_{i,j})_{i,j \in \mathbf{N}}$ by columns. For $n \in \mathbf{N}$, we set the n^{th} column of A equal to the $[0, 1]$ column of $(\tilde{J} - 1)^{-(n-1)}$. Then A satisfies (25), by construction. To compute the entries of A we invert \tilde{H} and its powers (22) to obtain

$$(\tilde{H})^{-1} = -t^{-1} \begin{bmatrix} t & -(1 + g(t)) \\ -g(t) & 0 \end{bmatrix}$$

and

$$(\tilde{H})^{-n} = (-1)^n t^{-n} \begin{bmatrix} h_n & -(1 + g(t))h_{n-1} \\ -g(t)h_{n-1} & th_{n-2} \end{bmatrix}, \quad n \geq 2.$$

Then we read off the coefficients of the appropriate powers of t in the first columns. The first two columns of A are given by

$$(26) \quad \begin{aligned} a_{i,1} &= \delta_{i,1}, & i \in \mathbf{N}, \\ a_{1,2} &= -1, & a_{2,2} = 1, & a_{i,2} = 0, & i \geq 3. \end{aligned}$$

For $m \geq 3$ and $s \geq 0$ we have

$$(27) \quad \begin{aligned} a_{2s+1,m} &= \text{coefficient of } t^{-s} \text{ in } (-1)^{m-1} t^{-(m-1)} h_{m-1} \\ &= (-1)^{m-1} \binom{m-s-1}{s} \\ a_{2s+2,m} &= \text{coefficient of } t^{-s} \text{ in } (-1)^m t^{-(m-1)} g(t) h_{m-2} \\ &= (-1)^m \sum_{k=1}^{\lfloor \frac{m}{2} \rfloor - s} b_k \binom{m-s-k-1}{s+k-1}. \end{aligned}$$

Let $Q = AJ_\infty = (q_{i,j})_{i,j \in \mathbf{N}}$. We check that Q has the properties (24). Since $\tilde{J}A = AJ_\infty$, it is clear that $\tilde{J}Q = QJ_\infty$. We have

$$(28) \quad q_{i,j} = \begin{cases} a_{i,j}, & \text{if } j = 1, \\ a_{i,j} + a_{i,j-1}, & \text{if } j \geq 2. \end{cases}$$

Since $a_{1,m} = (-1)^{m-1}$, it follows that $q_{1,j} = \delta_{1,j}$. Thus, $Q = P^{-1}$.

Finally, the entries of Q are obtained by applying (28) to (26) and (27). Thus, $q_{i,1} = \delta_{i,1}$ and $q_{i,2} = \delta_{i,2}$, for $i \in \mathbf{N}$. For $m \geq 3$ and $s \geq 0$, we have

$$(29) \quad \begin{aligned} q_{2s+1,m} &= (-1)^{m-1} \binom{m-s-2}{s-1} \\ q_{2s+2,m} &= (-1)^m \sum_{k=1}^{\lfloor \frac{m}{2} \rfloor - s} b_k \binom{m-s-k-2}{s+k-2}. \end{aligned}$$

Lemma 5.3. *For all i and j we have $|q_{i,j}| \leq 2^{3j}$ and $|p_{i,j}| \leq 2^{2j}$.*

Proof. The bound $|b_k| \leq 2^{2k-2}$ for $k \geq 1$ follows from (18). It is then elementary to verify the bounds of the lemma from the formulae (23) and (29). \square

Proof of Theorem 5.1. We define

$$\tau(Y) = P\tau_1(Y)P^{-1}, \quad Y \in \mathrm{SL}(2, \mathbf{Z}).$$

From its construction, τ satisfies conditions (a), (b) and (c) of Theorem 5.1. It follows from Lemma 5.3 that $\tau(S) = P\tilde{S}P^{-1}$ satisfies (d). \square

6. PROOF OF THEOREM 3.1

The matrix Z^{-1} studied in Section 4 is the transition matrix from the basis $\{e_n\}_{n \in \mathbf{N}}$ of E to a new basis $\{e'_n\}_{n \in \mathbf{N}}$. The linear transformation represented by the divisor matrix D in the basis $\{e_n\}_{n \in \mathbf{N}}$ is represented by J in the basis $\{e'_n\}_{n \in \mathbf{N}}$.

Since $\mathbf{N} = \bigcup_{d \text{ odd}} \{d2^{k-1} \mid k \in \mathbf{N}\}$ we have a decomposition

$$E = \bigoplus_{d \text{ odd}} E(d),$$

Where $E(d)$ is the subspace of E spanned by the elements $e'_{d2^{k-1}}$, $k \in \mathbf{N}$.

We consider the isomorphisms

$$\phi_d : E \rightarrow E(d), \quad e_k \mapsto e'_{d2^{k-1}}.$$

For each odd number d let $\mathcal{A}(d)$ be the subring of \mathcal{A} consisting of matrices whose entries $a_{i,j}$ are zero unless i and j both belong to the set $\{d2^{k-1} \mid k \in \mathbf{N}\}$.

The above isomorphisms induce isomorphisms

$$\psi_d : \mathcal{A} \rightarrow \mathcal{A}(d).$$

and a homomorphism

$$\psi : \mathcal{A} \rightarrow \prod_{d \text{ odd}} \mathcal{A}(d) \subseteq \mathcal{A}, \quad \psi(A) = (\psi_d(A))_{d \text{ odd}}$$

We have

$$\psi(J_\infty) = J.$$

Now for $A \in \mathcal{A}$, we have $\psi(A)_{i,j} = 0$ unless there exists an odd number d and $k, \ell \in \mathbf{N}$ with $(i, j) = (d2^{k-1}, d2^{\ell-1})$, in which case $\psi(A)_{i,j} = A_{k,\ell}$.

Let τ be the representation given by Theorem 5.1 and let $\tau(S) = (s_{k,\ell})_{k,\ell \in \mathbf{N}}$. By Theorem 5.1(a), $s_{k,\ell} = 0$ if $k > \ell + 1$. This means $\psi(\tau(S))_{i,j} = 0$ if $i > 2j$. By Theorem 5.1(d), there exists a constant C such that $|s_{k,\ell}| \leq 2^{C\ell}$, for all k and ℓ , which implies that $|\psi(\tau(S))_{i,j}| \leq 2^C j^C$, for all i and j . We conclude that $\psi(\tau(S)) \in \mathcal{DR}_0$. Since $\psi(\tau(T)) = J$, it follows that $\psi(\tau(\text{SL}(2, \mathbf{Z}))) \subseteq \mathcal{DR}_0$. Finally, the representation

$$\rho : \text{SL}(2, \mathbf{Z}) \rightarrow \mathcal{A}^\times, \quad Y \mapsto Z^{-1}\psi(\tau(Y))Z$$

satisfies all of the conditions of Theorem 3.1. The proof of Theorem 3.1 is now complete. \square

Remarks 6.1. By a closer examination of the proof we can strengthen the conclusions of Theorem 3.1 in the following ways. First, we have actually constructed the subgroup of \mathcal{DR}_0^\times isomorphic to the direct product of copies $\text{SL}(2, \mathbf{Z})$ (indexed by the odd numbers) with the

representation ρ conjugate to the diagonal embedding. Also part (d) can be sharpened to state that for $Y \in \mathrm{SL}(2, \mathbf{Z})$ we have $\rho(Y)_{i,j} = 0$ whenever $i > 2j$.

7. EXTENDING REPRESENTATIONS TO $\mathrm{GL}(2, \mathbf{Z})$

Let

$$W = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We have

$$(30) \quad W^2 = 1, \quad WSW = S^{-1}, \quad WRW = R^{-1}.$$

The relations (30) and (5) together form a set of defining relations for $\mathrm{GL}(2, \mathbf{Z}) = \langle \mathrm{SL}(2, \mathbf{Z}), W \rangle$.

In the following lemma the isomorphism γ is defined in (20) and the matrices $\gamma(\tilde{S})$, and $\gamma(\tilde{R})$ are from (21).

Lemma 7.1. *Let*

$$W(t) = \frac{1}{\sqrt{t^2 + 4t + 1}} \begin{bmatrix} -t & 2g(t) + 1 \\ 2g(t) + 1 & t \end{bmatrix}.$$

Then $W(t)$ is, up to a sign, the unique element of $\mathrm{GL}(2, \mathbf{C}[[t]])$ such that

- (i) $W(t)^2 = 1$.
- (ii) $W(t)\gamma(\tilde{S})W(t) = \gamma(\tilde{S})^{-1}$
- (iii) $W(t)\gamma(\tilde{R})W(t) = \gamma(\tilde{R})^{-1}$
- (iv) $W(0) = W$.

Proof. The proof is straightforward, by matrix calculations in $M_2(\mathbf{C}[[t]])$, using the relation (17). \square

Lemma 7.2. *For $i, j \in \{1, 2\}$, let $w_{i,j}(t) = \sum_{n=0}^{\infty} r_n t^n$. Then there exists a constant C , such that $|r_n| \leq 2^{Cn}$.*

Proof. We consider those power series $\sum_{n=0}^{\infty} s_n t^n$ with real coefficients for which there exists a constant D , which may depend on the series, such that $|s_n| \leq 2^{Dn}$. We observe that the product of two such series has the same property. Since $g(t)$ has this property and since $t^2 + 4t + 1 = (t + (2 + \sqrt{3}))(t + (2 - \sqrt{3}))$, we are reduced to proving the bound for the Taylor series, centered at 0, of $f(t) = (t + a)^{-\frac{1}{2}}$, where $a > 0$. We have

$$f^{(n)}(t) = (-1)^n \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2^n} (t + a)^{-\frac{(2n+1)}{2}},$$

Hence,

$$\left| \frac{f^{(n)}(0)}{n!} \right| = \frac{1}{2^{2n}} \binom{2n}{n} a^{-\frac{(2n+1)}{2}} \leq \frac{1}{\sqrt{a}} \left(\frac{1}{a}\right)^n.$$

□

Proposition 7.3. *The representation $\rho : \mathrm{SL}(2, \mathbf{Z}) \rightarrow \mathcal{DR}_0^\times$ can be extended to $\mathrm{GL}(2, \mathbf{Z})$.*

Proof. Set $\tilde{W} = \gamma^{-1}(W(t))$. Then by Lemma 7.1, the group generated by \tilde{S} , \tilde{R} and \tilde{W} is isomorphic to $\mathrm{GL}(2, \mathbf{Z})$ and we can extend the representation τ_1 from $\mathrm{SL}(2, \mathbf{Z})$ to $\mathrm{GL}(2, \mathbf{Z})$ by setting $\tau_1(W) = \tilde{W}$. Hence we can also extend the representations τ and ρ by setting $\tau(W) = P\tau_1(W)P^{-1}$ and $\rho(W) = Z^{-1}\psi(\tau(W))Z$. Then Lemma 7.2 and Lemma 5.3 imply that $\rho(\mathrm{GL}(2, \mathbf{Z})) \subseteq \mathcal{DR}_0$. □

Remark 7.4. Note that $\tau_1(W)$, $\tau(W)$ and $\rho(W)$ are not integral matrices.

8. UNIQUENESS OF M_∞

Let S and T be the generators of $G = \mathrm{SL}(2, \mathbf{Z})$ as given in (4). Let V denote the standard 2-dimensional $\mathbf{C}G$ -module.

We shall call a $\mathbf{C}G$ -module *T -indecomposable module* if T acts indecomposably and unipotently on every T -invariant subspace. One example is the $\mathbf{C}G$ -module, which we shall denote by M_∞ , defined by the representation τ of Theorem 5.1.

Theorem 8.1. *M_∞ is the unique T -indecomposable $\mathbf{C}G$ -module which has an ascending filtration $\{M_n\}_{n \in \mathbf{N}}$ in which every quotient M_n/M_{n-1} is isomorphic to V .*

Some lemmas are needed for the proof of Theorem 8.1.

Lemma 8.2. $\mathrm{Ext}_{\mathbf{C}G}^1(V, V) \cong \mathbf{C}$.

Proof. Suppose we have a module extension M of V by itself and let $\mu : G \rightarrow \mathrm{GL}(M)$ denote the representation. Since the cyclic group $\langle ST \rangle$ of order 6 acts semisimply, we may choose a basis of M such that

$$\mu(ST) = \begin{bmatrix} ST & 0 \\ 0 & ST \end{bmatrix} \quad \text{and} \quad \mu(S) = \begin{bmatrix} S & z(S) \\ 0 & S \end{bmatrix},$$

for some 2×2 matrix $z(S)$. Since $\mu(S)^2 = -I$, we have $z(S)S + Sz(S) = 0$, so

$$z(S) = \begin{bmatrix} a & b \\ b & -a \end{bmatrix}$$

for some $a, b \in \mathbf{C}$.

By a further change of basis we can reduce to

$$\mu(S) = \begin{bmatrix} 0 & -1 & a & 0 \\ 1 & 0 & 0 & -a \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

while leaving $\mu(ST)$ unchanged. Thus, $\dim \mathrm{Ext}_{\mathbf{CG}}^1(V, V) \leq 1$. Lastly, if $a \neq 0$ then $\mu(T) = -\mu(S)\mu(ST)$ acts indecomposably. \square

Lemma 8.3. *For each natural number n there is, up to isomorphism, a unique T -indecomposable \mathbf{CG} -module $M(n)$ of length n and having all composition factors isomorphic to V .*

Proof. We already have existence of such a module, as a submodule of M_∞ . We prove by induction that $\mathrm{Ext}_{\mathbf{CG}}^1(V, M(k)) \cong \mathbf{Q}$. The case $k = 1$ is Lemma 8.2. We apply $\mathrm{Hom}_{\mathbf{CG}}(V, -)$ to the short exact sequence

$$0 \rightarrow M(k-1) \rightarrow M(k) \rightarrow V \rightarrow 0.$$

The long exact sequence of cohomology is:

$$\begin{aligned} 0 \rightarrow \mathrm{Hom}_{\mathbf{CG}}(V, M(k-1)) &\rightarrow \mathrm{Hom}_{\mathbf{CG}}(V, M(k)) \rightarrow \mathrm{Hom}_{\mathbf{CG}}(V, V) \\ &\rightarrow \mathrm{Ext}_{\mathbf{CG}}^1(V, M(k-1)) \rightarrow \mathrm{Ext}_{\mathbf{CG}}^1(V, M(k)) \rightarrow \mathrm{Ext}_{\mathbf{CG}}^1(V, V) \rightarrow \end{aligned}$$

The desired conclusion follows by induction and Lemma 8.2. \square

Lemma 8.4. *Let M, M' be isomorphic to $M(n)$ and let N, N' be their maximal \mathbf{CG} -submodules. Then any \mathbf{CG} -isomorphism from N to N' can be extended to an isomorphism from M to M' .*

Proof. We argue by induction on n , the case $n = 1$ being trivial. We assume $n > 1$. By Lemma 8.3, N' has, for each $k \leq n-1$, a unique submodule $N'(k) \cong M(k)$ of length k and these are all the submodules of N' . Let $\psi : N \rightarrow N'$ be a given isomorphism. Choose any isomorphism $\phi : M \rightarrow M'$. Replacing ϕ by a scalar multiple, we can assume that $\alpha := \phi|_N - \psi \in \mathrm{Hom}_{\mathbf{CG}}(N, N')$ is not an isomorphism, so it has a nonzero kernel K . Hence α induces an isomorphism $N/K \rightarrow N'(k)$ for some $k < n-1$. By induction, this isomorphism may be extended to an isomorphism $\bar{\beta} : M/K \rightarrow N'(k+1)$. The induced map $\beta : M \rightarrow N'(k+1)$ is an extension of α . Thus, ψ extends to $\phi - \beta$, which is an isomorphism, since $N'(k+1) \subsetneq M'$. \square

Proof of Theorem 8.1. Let M_∞ and M'_∞ be modules satisfying the conditions of Theorem 8.1. Then the submodules M_n and M'_n in their respective filtrations are isomorphic with $M(n)$. By Lemma 8.4 we can define isomorphisms $\phi_n : M_n \rightarrow M'_n$ recursively for $n \in \mathbf{N}$, so that ϕ_{n+1} extends ϕ_n . We can therefore define $\phi : M_\infty \rightarrow M'_\infty$ as follows. Each

$m \in M_\infty$. belongs to M_n for some n . By the extension property, $\phi_n(m)$ does not depend on n , so we can define a map ϕ by $\phi(m) = \phi_n(m)$, which is easily seen to be an isomorphism. \square

9. DIRICHLET SERIES IN THE $\mathrm{SL}(2, \mathbf{Z})$ -ORBIT OF $\zeta(s)$

We may identify \mathcal{DS} with $\mathcal{D}\{s\}$ and consider the action of $\mathrm{SL}(2, \mathbf{Z})$ on analytic Dirichlet series via ρ . We denote the Dirichlet series with one term 1^{-s} simply by 1. We have $1.\rho(T) = \zeta(s)$. We set $\varphi(s) := 1.\rho(-S)$ and write

$$\varphi(s) := \sum_{n=1}^{\infty} a_n n^{-s},$$

where $a_n = \rho(-S)_{1,n}$. We denote the abscissae of conditional and absolute convergence of $\varphi(s)$ by σ_c and σ_a , respectively.

Let $\mathbf{C}(\zeta(s), \varphi(s))$ be the subfield of the field of meromorphic functions of the half-plane $\mathrm{Re}(s) > \max(1, \sigma_c)$ generated by the functions $\zeta(s)$ and $\varphi(s)$. It will be shown below that the Dirichlet series in the orbit $1.\rho(\mathrm{SL}(2, \mathbf{Z}))$ all converge in this half-plane and that the analytic functions they define belong to $\mathbf{C}(\zeta(s), \varphi(s))$. Let $\mathbf{Z}G$ denote the integral group ring. The representation ρ extends uniquely to a ring homomorphism from $\mathbf{Z}G$ to \mathcal{A} , which we will denote by ρ also. The kernel of this homomorphism contains the 2-sided ideal Q generated by the elements $S + S^{-1}$ and $R + R^{-1} - 1$. Since $R = ST$, we have the relation

$$TS = 1 + ST^{-1}$$

in $\mathbf{Z}G/Q$. It follows that $\mathbf{Z}G/Q$ and hence $\rho(\mathbf{Z}G)$ is generated as an abelian group by the images of the elements T^m and ST^m , $m \in \mathbf{Z}$.

Theorem 9.1. *The Dirichlet series in the common $\mathrm{SL}(2, \mathbf{Z})$ -orbit of 1, $\zeta(s)$ and $\varphi(s)$ all converge for $\mathrm{Re}(s) > \max(1, \sigma_c)$, and belong to the additive subgroup of $\mathbf{C}(\zeta(s), \varphi(s))$ generated by the elements $\zeta(s)^m$ and $\varphi(s)\zeta(s)^m$, $m \in \mathbf{Z}$.*

Proof. We first note that $\zeta(s)$ has no zeros in the half-plane $\mathrm{Re}(s) > \max(1, \sigma_c)$ and that $\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \mu(n)n^{-s}$, converges absolutely there. Here, $\mu(n)$ is the Möbius function. In this half-plane we have $1.\rho(T^m) = 1.D^m = \zeta(s)^m$ and $1.\rho(ST^m) = 1.\rho(S)\rho(T^m) = -\varphi(s)\zeta(s)^m$, for every $m \in \mathbf{Z}$. The theorem now follows from the discussion preceding it. \square

10. THE CUBIC EQUATION RELATING $\zeta(s)$ AND $\varphi(s)$

Let $\mathbf{N}_0 = \mathbf{N} \cup \{0\}$ be the set of nonnegative integers.

Lemma 10.1. *We have*

$$a_n = \rho(-S)_{1,n} = \alpha_1(n) + \sum_{\ell \geq 4} (-1)^\ell \alpha_{\ell-1}(n) \sum_{k=2}^{\lfloor \frac{\ell}{2} \rfloor} b_k \binom{\ell - k - 2}{k - 2}.$$

(See Section 4 and formula (16) for the definitions of $\alpha_k(n)$ and b_k .)

Proof. This is computed directly from the general formula for ρ :

$$\rho(-S) = Z^{-1} \psi(P\tau_1(-S)P^{-1})Z.$$

We recall the following information.

- (a) The matrix $\tau_1(-S)$ is the block-diagonal matrix with the 2×2 block $-S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ repeated along the main diagonal. (Lemma 5.2)
- (b) The first rows of Z^{-1} and P are equal to the first row of the identity matrix. (Lemma 4.5 and Section 5.1.)
- (c) For $A = (a_{i,j})_{i,j \in \mathbf{N}}$, we have $\psi(A)_{i,j} = 0$ unless there exist $k, \ell \in \mathbf{N}$ and an odd number d such that $(i, j) = (2^{k-1}d, 2^{\ell-1}d)$, in which case $\psi(A)_{i,j} = a_{k,\ell}$. (Section 6.)
- (d) From formula (29) the entries in the second row of $P^{-1} = (q_{k,\ell})$ are given by $q_{2,1} = 0$, $q_{2,2} = 1$ and, for $\ell \geq 3$,

$$(31) \quad q_{2,\ell} = (-1)^\ell \sum_{k=2}^{\lfloor \frac{\ell}{2} \rfloor} b_k \binom{\ell - k - 2}{k - 2}.$$

- (e) The entries of the matrix $Z = (\alpha(i, j))_{i,j \in \mathbf{N}}$ satisfy the equation $\alpha(2^r, j) = \alpha_r(j)$, for $r \in \mathbf{N}$. (Lemma 4.5.)

By (b), the first row of $\rho(-S)$ is obtained by multiplying the first row of $\psi(P\tau_1(-S)P^{-1})$ with Z . By (c), the only nonzero entries in the first row of $\psi(P\tau_1(-S)P^{-1})$ are the entries $\psi(P\tau_1(-S)P^{-1})_{1,2^{\ell-1}} = (P\tau_1(-S)P^{-1})_{1,\ell}$, for $\ell \in \mathbf{N}$. Then by (b) and (a),

$$(32) \quad (P\tau_1(-S)P^{-1})_{1,\ell} = (\tau_1(-S)P^{-1})_{1,\ell} = q_{2,\ell}.$$

Hence, by (e) and (d),

$$(33) \quad \begin{aligned} a_n &= \sum_{\ell \in \mathbf{N}} q_{2,\ell} \alpha(2^{\ell-1}, n) \\ &= \alpha_1(n) + \sum_{\ell \geq 3} q_{2,\ell} \alpha_{\ell-1}(n), \end{aligned}$$

and the lemma follows since $q_{2,3} = 0$, by (d). \square

Let $\Omega = \{p_1, \dots, p_r\}$ be a finite set primes and let t_1, \dots, t_r be indeterminates. We will be interested in the formal power series

$$F_\Omega = \sum_{(n_1, \dots, n_r) \in \mathbf{N}_0^r} a_{p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}} t_1^{n_1} \dots t_r^{n_r}.$$

Let

$$y = \frac{1}{(1-t_1)(1-t_2)\dots(1-t_r)} - 1 = \sum_{(n_1, \dots, n_r) \in \mathbf{N}_0^r} \alpha_1(p_1^{n_1} \dots p_r^{n_r}) t_1^{n_1} \dots t_r^{n_r}.$$

Then for $\ell \geq 1$

$$y^\ell = \sum_{(n_1, \dots, n_r) \in \mathbf{N}_0^r} \alpha_\ell(p_1^{n_1} \dots p_r^{n_r}) t_1^{n_1} \dots t_r^{n_r}.$$

Then we have

$$\begin{aligned} \frac{-y}{1+y} &= \sum_{\ell \in \mathbf{N}} (-1)^\ell y^\ell \\ (34) \quad &= \sum_{(n_1, \dots, n_r) \in \mathbf{N}_0^r} \left[\sum_{\ell \in \mathbf{N}} (-1)^\ell \alpha_\ell(p_1^{n_1} \dots p_r^{n_r}) \right] t_1^{n_1} \dots t_r^{n_r}. \end{aligned}$$

Set

$$\begin{aligned} f_\Omega &= \sum_{(n_1, \dots, n_r) \in \mathbf{N}_0} \sum_{\ell \in \mathbf{N}} (-1)^\ell \alpha_{\ell-1}(p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}) \sum_{k=2}^{\lfloor \frac{\ell}{2} \rfloor} b_k \binom{\ell-k-2}{k-2} t_1^{n_1} \dots t_r^{n_r} \\ &= \sum_{\ell \in \mathbf{N}} \sum_{k=2}^{\lfloor \frac{\ell}{2} \rfloor} b_k (-1)^\ell \binom{\ell-k-2}{k-2} y^{\ell-1} \\ &= \sum_{k \geq 2} \left[\sum_{\ell \geq 2k} (-1)^\ell \binom{\ell-k-2}{k-2} y^{\ell-1} \right] b_k. \end{aligned}$$

By Lemma 10.1,

$$F_\Omega = y + f_\Omega.$$

For $k \geq 2$ we set

$$C_k = \sum_{\ell \geq 2k} (-1)^\ell \binom{\ell-k-2}{k-2} y^{\ell-1}$$

so that

$$f_\Omega = \sum_{k \geq 2} b_k C_k.$$

Next we consider, for $k \in \mathbf{N} \setminus \{1\}$, the generalized binomial coefficients

$$p_k(x) = \frac{(x-k-2)(x-k-3)\dots(x-2k+1)}{(k-2)!}$$

as polynomials in x of degree $k - 2$. Note that $p_k(\ell) = \binom{\ell-k-2}{k-2}$ for ℓ an integer $\geq 2k$ but, for example, when $\ell - k - 2$ is a negative integer, the value $p_k(\ell)$ may be nonzero, whereas our convention concerning binomial coefficients would say that $\binom{\ell-k-2}{k-2} = 0$. In order to find C_2 and C_3 , we shall evaluate

$$\widehat{C}_k = \sum_{\ell \in \mathbf{N}} (-1)^\ell p_k(\ell) y^\ell.$$

For $k = 2$, we have $p_2(\ell) = 1$, so $\widehat{C}_2 = \frac{-y}{1+y}$ by (34). Hence

$$(35) \quad C_2 = \frac{-1}{1+y} - \sum_{\ell=1}^3 (-1)^\ell y^{\ell-1} = \frac{-1}{1+y} + 1 - y + y^2 = \frac{y^3}{1+y}.$$

For $k = 3$, we have $p_3(\ell) = \ell - 5$, so

$$(36) \quad \begin{aligned} \widehat{C}_3 &= \sum_{\ell \in \mathbf{N}} (-1)^\ell \ell y^\ell - 5 \sum_{\ell \in \mathbf{N}} (-1)^\ell y^\ell \\ &= \left(\frac{-y}{1+y} + \frac{y^2}{(1+y)^2} \right) + 5 \frac{y}{1+y} \\ &= \frac{4y}{1+y} + \frac{y^2}{(1+y)^2}, \end{aligned}$$

where the second equality is obtained by applying the operator $y \frac{d}{dy}$ to the first and second members of (34). Therefore,

$$(37) \quad \begin{aligned} C_3 &= \frac{4}{1+y} + \frac{y}{(1+y)^2} - [(-1)p_3(1) + p_3(2)y - p_3(3)y^2 + p_3(4)y^3] \\ &= \frac{4}{1+y} + \frac{y}{(1+y)^2} - 4 + 3y - 2y^2 + y^3 \\ &= \frac{y^5}{(1+y)^2}. \end{aligned}$$

Suppose $k \geq 3$. We have

$$\begin{aligned} C_k &= y^{2k-1} + \sum_{\ell \geq 2k+1} (-1)^\ell \binom{\ell-k-2}{k-2} y^{\ell-1} \\ &= y^{2k-1} + \sum_{\ell \geq 2k+1} (-1)^\ell \binom{\ell-1-k-2}{k-2} y^{\ell-1} + \sum_{\ell \geq 2k+1} (-1)^\ell \binom{\ell-1-k-2}{k-3} y^{\ell-1}. \end{aligned}$$

Set

$$A = \sum_{\ell \geq 2k+1} (-1)^\ell \binom{\ell-1-k-2}{k-2} y^{\ell-1}, \quad B = \sum_{\ell \geq 2k+1} (-1)^\ell \binom{\ell-1-k-2}{k-3} y^{\ell-1}.$$

In A , set $\ell' = \ell - 1$ and in B , set $k' = k - 1$. Then

$$A = -yC_k, \quad B = y^2C_{k-1} - y^{2k-1}$$

Thus,

$$C_k = y^{2k-1} + A + B = y^{2k-1} - yC_k + y^2C_{k-1} - y^{2k-1} = -yC_k + y^2C_{k-1}.$$

Therefore,

$$C_k = \frac{y^2}{1+y}C_{k-1}, \quad \text{with } C_2 = \frac{y^3}{1+y}$$

so

$$C_k = \frac{y^{2k-1}}{(1+y)^{k-1}}.$$

Hence

$$\begin{aligned} \frac{C_k C_{k'}}{C_{k+k'}} &= \frac{y^{2(k+k')-2}}{(1+y)^{k+k'-2}} \cdot \frac{(1+y)^{k+k'-1}}{y^{2(k+k')-1}} = \frac{1+y}{y}. \\ f_\Omega^2 &= \left(\sum_{k \geq 2} b_k C_k \right)^2 = \sum_{k, k' \geq 2} b_k b_{k'} C_{k+k'} \frac{(1+y)}{y} \end{aligned}$$

Then, from the definition (16) of the b_k ,

$$\begin{aligned} \frac{y}{1+y} f_\Omega^2 &= \sum_{K \geq 4} \left(\sum_{k=2}^{K-2} b_k b_{K-k} \right) C_K \\ &= \sum_{K \geq 4} (-b_K - 2b_{K-1}) C_K \\ &= - \sum_{K \geq 2} b_K C_K + b_2 C_2 + b_3 C_3 - 2 \frac{y^2}{1+y} \sum_{L \geq 3} b_L C_L \\ &= -f_\Omega - C_2 + 2C_3 - \frac{2y^2}{1+y} f_\Omega - \frac{2y^2}{1+y} C_2 \\ &= -\left(1 + \frac{2y^2}{1+y}\right) f_\Omega - \frac{y^3}{1+y} + \frac{2y^5}{(1+y)^2} - \frac{2y^2}{1+y} \cdot \frac{y^3}{1+y}. \end{aligned}$$

Therefore, we have

$$(38) \quad y f_\Omega^2 + (1+y+2y^2) f_\Omega + y^3 = 0.$$

Since $F_\Omega = f_\Omega + y$, this yields

$$(39) \quad y F_\Omega^2 + (1+y) F_\Omega - y(1+y) = 0.$$

Set

$$(40) \quad P(z, w) = zw^2 + (1+z)w - z(1+z)$$

The discriminant $\Delta(z)$ is equal to $(1+z)^2 + 4z^2(1+z)$. Set $c = \min\{|e| \mid e \in \mathbf{C} \text{ and } \Delta(e) = 0\}$. Then there is a formal power series

$u = \sum_{n=0}^{\infty} \gamma_n z^n$ such that $P(z, u) = 0$ and u defines an analytic function in $\{z \in \mathbf{C} \mid |z| < c\}$. Now the roots of $\Delta(z)$ are -1 and $e, \bar{e} = \frac{-1 \pm \sqrt{-15}}{8}$. Since $|e| = \frac{1}{2}$, it follows that u converges for $|z| < \frac{1}{2}$. Applied to (39), we see that if t_i take complex values with $|\prod_{i=1}^r \frac{1}{1-t_i} - 1| < \frac{1}{2}$, the power series F_{Ω} converges. In particular for $s \in \mathbf{C}$ with sufficiently large real part, we have convergence when we set the $t_i = p_i^{-s}$. If we denote by \mathbf{N}_{Ω} the set of natural numbers for which every prime factor belongs to Ω , and define

$$(41) \quad \varphi_{\Omega}(s) = \sum_{n \in \mathbf{N}_{\Omega}} a_n n^{-s}, \quad \text{and} \quad \zeta_{\Omega}(s) = \sum_{n \in \mathbf{N}_{\Omega}} n^{-s},$$

we obtain the equation

$$(42) \quad (\zeta_{\Omega}(s) - 1)\varphi_{\Omega}(s)^2 + \zeta_{\Omega}(s)\varphi_{\Omega}(s) - \zeta_{\Omega}(s)(\zeta_{\Omega}(s) - 1) = 0.$$

Initially, we know that this equation holds for s with sufficiently large real part. The Dirichlet series $\zeta_{\Omega}(s)$ and $\varphi_{\Omega}(s)$ converge absolutely in the half-plane $\text{Re}(s) > \max(1, \sigma_a)$, where both $\zeta(s)$ and $\varphi(s)$ converge absolutely. It is then a general property of Dirichlet series that they converge uniformly on compact subsets of this half-plane, defining analytic functions there. Then, by the principle of analytic continuation, the equation (42) holds in this half-plane. If we take Ω to be the set of the first r primes and allow r to increase, the resulting sequences of analytic functions $\zeta_{\Omega}(s)$ and $\varphi_{\Omega}(s)$ defined in the above half-plane converge to $\zeta(s)$ and $\varphi(s)$, respectively.

Theorem 10.2. *In the half plane $\text{Re}(s) > \max(1, \sigma_c)$, we have*

$$(43) \quad (\zeta(s) - 1)\varphi(s)^2 + \zeta(s)\varphi(s) - \zeta(s)(\zeta(s) - 1) = 0.$$

Proof. The validity of this algebraic relation for $\text{Re}(s) > \max(1, \sigma_a)$ is immediate from the foregoing discussion. Since $\zeta(s)$ and $\varphi(s)$ represent analytic functions throughout the half-plane $\text{Re}(s) > \max(1, \sigma_c)$ the relation is valid on this larger region, by the principle of analytic continuation. \square

Remark 10.3. Since $\phi(s)$ defines an analytic function in $\text{Re}(s) > \sigma_c$, it follows that $\zeta(s) - 1$ cannot be equal to any root of $\Delta(z)$ for s in this half-plane. By Theorem 11.6 (C) of [3], $\zeta(s)$ takes on every nonzero value in $\text{Re}(s) > 1$. Therefore, $\sigma_c > 1$. A sharper bound follows from [4], which proves the existence of a constant $C \approx 1.764$ such that the closure $M(\sigma)$ of the set of values of $-\log \zeta(\sigma + it)$, $t \in \mathbf{R}$, is bounded by a convex curve when $\sigma < C$, and a ring-shaped domain between two convex curves when $\sigma > C$. From this it follows by computation that $\zeta(s) = \frac{7 \pm \sqrt{-15}}{8}$ for some s with $\text{Re}(s)$ arbitrarily close to 1.8, so

$\sigma_c \geq 1.8$. We also know from the results of [3], p.300, that $\zeta(s)$ never takes the value $\frac{-7 \pm \sqrt{-15}}{8}$ when $\operatorname{Re}(s) > 1.92$.

Remark 10.4. A slight modification of the discussion above shows that (42) holds for an arbitrary set Ω of primes, again for $\operatorname{Re}(s) > \sigma_a$.

The function $\zeta(s)$ can be extended to a meromorphic function in the whole complex plane, whose only singularity is a simple pole at $s = 1$. Then equation (43) defines analytic continuations of $\varphi(s)$ along arcs in the plane which do not pass through $s = 1$ or the branch points $\{s \mid \zeta(s) = 0 \text{ or } \frac{7 \pm \sqrt{-15}}{8}\}$, with the exception that one of the two branches at each point s with $\zeta(s) = 1$ has a simple pole there. By [4], we know that there is a constant $C \approx 1.764$ such that $\zeta(s) \neq 1$ for all s with $\operatorname{Re}(s) > C$.

10.1. Some generalizations. In the discussion following (40), we could equally well have substituted $t_i = M(p_i)p_i^{-s}$, where M is any bounded, completely multiplicative complex function of the natural numbers, such as a Dirichlet character. In that case, if we set

$$(44) \quad \zeta_M(s) = \sum_{n=1}^{\infty} M(n)n^{-s}, \quad \varphi_M(s) = \sum_{n=1}^{\infty} a_n M(n)n^{-s},$$

the same reasoning shows that $\zeta_M(s)$ and $\varphi_M(s)$ are related by (43), just as $\zeta(s)$ and $\varphi(s)$ are, in a suitable half-plane.

We can also extend our discussion to number fields. For this purpose, a necessary remark is that, by Lemma 10.1, the coefficient a_n in $\varphi(s)$ depends only on the partition $\lambda : e_1 \geq e_2 \geq \cdots \geq e_r \geq 1$ defined by the exponents e_i which occur in the prime factorization of n , in that if n and n' define the same partition then $a_n = a_{n'}$. We write a_λ for this common value.

Let K be a number field. The factorization of an ideal \mathfrak{g} of its ring of integers \mathfrak{o} into prime ideals determines a partition λ , so we may set $a_{\mathfrak{g}} = a_\lambda$. With these notations, our previous discussion up to (40) remains valid if the set Ω is taken to be a finite set $\{\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_r\}$ of prime ideals in \mathfrak{o} , instead of rational primes. Then, in the paragraph following (40), if we substitute $t_i = N(\mathfrak{P}_i)^{-s}$, we deduce, as before, that the Dedekind zeta function of K ,

$$(45) \quad \zeta_K(s) = \sum_{\mathfrak{g}} N(\mathfrak{g})^{-s}$$

is related to the Dirichlet series

$$(46) \quad \varphi_K(s) = \sum_{\mathfrak{g}} a_{\mathfrak{g}} N(\mathfrak{g})^{-s}$$

by the cubic relation (43), in the appropriate half-plane.

11. A FUNCTIONAL EQUATION FOR $\varphi(s)$

The classical functional equation for $\zeta(s)$ can be written as

$$(47) \quad \zeta(1-s) = a(s)\zeta(s),$$

where $a(s) = \frac{\Gamma(s/2)\pi^{-s/2}}{\Gamma((1-s)/2)\pi^{-(1-s)/2}}$.

If we apply this to (43) with s replaced by $(1-s)$ and then eliminate $\zeta(s)$ from the resulting equation, using (43), a functional equation relating $\varphi(s)$ and $\varphi(1-s)$ is obtained. Let

$$(48) \quad G(a, x, y) = a^4 x^4 - a^3 x^2 (x^2 + x + 1)(y^2 + y + 1) \\ + a^2 [x^2 (y^2 + y + 1)^2 + y^2 (x^2 + x + 1)^2 - 2x^2 y^2] \\ - ay^2 (x^2 + x + 1)(y^2 + y + 1) + y^4.$$

Then $G(a, x, y)$ is irreducible in $\mathbf{C}[a, x, y]$ and $G(a(s), \varphi(s), \varphi(1-s)) = 0$.

Acknowledgements. We thank Peter Sarnak for some helpful discussions and for bringing [1] to our attention.

REFERENCES

- [1] Ju. V. Linnik, “The Dispersion Method in Binary Additive Problems”, Translations of Mathematical Monographs, Vol. 4, American Mathematical Society, Providence, Rhode Island, 1963.
- [2] L. Solomon, The orders of the finite Chevalley groups, *J. Algebra* **3** (1966) 376–393.
- [3] E. C. Titchmarsh, “The theory of the Riemann zeta-function”, Second edition. Edited and with a preface by D. R. Heath-Brown. The Clarendon Press, Oxford University Press, New York, 1986.
- [4] H. Bohr and B. Jessen, On the Distribution of the Values of the Riemann Zeta Function, *American Journal of Mathematics* 58, (1936), No. 1, 35–44.
- [5] J. G. Thompson, The Divisor Matrix and $SL(2, \mathbf{Z})$, Preprint, University of Florida, (2007).
- [6] F. Bayart, A. Mouze, Factorialité de l’anneau des séries de Dirichlet analytiques, *C. R. Acad. Sci. Paris, Ser. I* 336 (2003).
- [7] A. Ostrowski, Über Dirichletsche Reihen und algebraische Differentialgleichungen, *Math Z.* 8 (1920), 241–298.
- [8] R. Redheffer, Eine explizit lösbare Optimierungsaufgabe. (German) Numerische Methoden bei Optimierungsaufgaben, Band 3 (Tagung, Math. Forschungsinst., Oberwolfach, 1976), pp. 213–216. Internat. Ser. Numer. Math., Vol. 36, Birkhäuser, Basel, 1977.
- [9] Vaughan, R. C. On the eigenvalues of Redheffer’s matrix. II. *J. Austral. Math. Soc. Ser. A* 60 (1996), no. 2, 260–273.

- [10] Vaughan, R. C. On the eigenvalues of Redheffer's matrix. I. Number theory with an emphasis on the Markoff spectrum (Provo, UT, 1991), 283–296, Lecture Notes in Pure and Appl. Math., 147, Dekker, New York, 1993.
- [11] Barrett, Wayne W. ; Jarvis, Tyler J. Spectral properties of a matrix of Redheffer. Directions in matrix theory (Auburn, AL, 1990). Linear Algebra Appl. 162/164 (1992), 673–683.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF FLORIDA, PO Box 118105,
GAINESVILLE, FL 32611–8105, USA

E-mail address: `sin@math.ufl.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF FLORIDA, PO Box 118105,
GAINESVILLE, FL 32611–8105, USA

E-mail address: `jthompso@math.ufl.edu`